

能链智电 (NASDAQ: NAAS) 负责任人工智能政策

一、目的与适用范围

浙江安吉智电控股有限公司（以下简称“能链智电”或“公司”）坚守**以人为本、负责任应用 AI** 的基本准则，将人工智能伦理规范、数据安全与人机协同发展纳入统一的 AI 治理框架，平衡技术创新价值与各利益相关方权益。本政策适用于公司及其子公司、分支机构以及代表公司开展业务的全体人员，覆盖自主研发的 NEF (NaaS Energy Fintech) 能源数字化 AI 系统及算法矩阵，以及经营活动中选用的全部第三方 AI 模型、工具与平台，涵盖 AI 的规划、开发、采购、部署、运营、退役全生命周期。

本政策依据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《生成式人工智能服务管理暂行办法》等法律法规制定，并参照经济合作与发展组织 (OECD) 人工智能原则、联合国教科文组织《人工智能伦理问题建议书》、欧盟《人工智能法案》(EU AI Act) 及 ISO/IEC 42001 人工智能管理体系标准的框架要求。本政策由公司董事会审议批准，自批准之日起生效。公司全体董事、管理层及员工均须遵守本政策。

二、AI 治理架构与职责

2.1 公司建立自上而下分层的 AI 治理体系：董事会作为最高决策机构批准并背书本政策、审议 AI 战略及重大风险事项；高级管理层统筹 AI 战略落地，其中首席技术官 (CTO) 为人工智能治理的最高管理责任人，兼任数据安全委员会主席，直接向首席执行官 (CEO) 及董事会汇报；数据安全委员会审议 AI 相关的数据使用、隐私保护与风险管控规范并审定重大 AI 应用上线；各业务部门为执行责任主体，落实场景落地、日常监督与风险上报；人力资源部门承担员工 AI 能力培育与伦理文化传播；合规与法务部门负责法规跟踪、合规审查与违规处置。

2.2 公司建立 AI 应用分级分类管理机制，按场景风险等级确定审批层级与监督频率，高风险场景须经数据安全委员会审议。

三、负责任人工智能基本原则

3.1 尊重数据隐私：公司在 AI 开发与使用全过程中保护个人数据，严格遵守适用的数据保护法律法规。系统搭建全流程数据治理链路，数据均经脱敏处理，仅用于业务经营与能源调度；公司实行数据分类分级管理，对敏感数据建立访问行为审计记录，对外共享数据一律经外发审批。AI 训练与推理遵循合法、正当、必要和最小化原则，禁止将用户个人数据用于未经授权用途。

3.2 保障 AI 系统网络安全：公司对 AI 系统及其支撑基础设施实施多层次防护，包括数据库审计与异常行为预警、数据防泄漏 (DLP) 系统、传输与存储加密、安全编码规范，以及系统上线前的漏洞扫描与渗透测试。AI 系统纳入《数据安全事件应急管理规范》覆盖范围，建立“事件研判—溯源排查—整改补救—复盘审计—出具结案报告”的闭环应急响应流程；针对生成式 AI 应用采取输入内容过滤与提示词防护 (prompt shield)，防止有害或不适当内容的生成与传播。

3.3 避免潜在偏见：公司要求 AI 系统的设计与训练确保公平、非歧视的行为结果：在数据训练环节识别并缓解数据源与标注偏见，优先采用多样化、具有代表性的训练数据集；定期开展偏见测试与公平性评估，检查模型在不同群体间是否存在差异化处置；对发现的偏见风险采取数据补正、模型调优或限制应用范围等措施予以纠正。

3.4 人类在环与人工干预：公司坚持“人为决策主体，AI 仅作为辅助工具”，关键业务判断的 AI 输出必须由人工复核，AI 生成内容须经人工确认后方可对外使用，AI 系统不得在无人工监督的情况下作出不可逆或高风险决策。根据 AI 应用的风



能链智电官方公众号

请扫码关注

险等级，选择适用以下一种或多种人类监督形式：人工决策（human-in-command，保留最终决定权）、人工监督（human-on-the-loop，持续监控）与人工审批（human-in-the-loop，输出须经批准）；相关人员有权干预、覆盖、中止或升级 AI 决策并保留记录。

3.5 透明度与可解释性：公司在对外披露与内部告知中说明 AI 的使用场景、能力范围、局限性、数据来源与潜在风险；涉及用户交互时主动告知用户其交互对象为 AI 系统而非人工；对影响相关方权益的 AI 驱动决策提供可理解的结果说明与依据阐释，详细程度与相关方需求及决策影响程度相匹配。

3.6 明确问责：公司为 AI 成果、风险决策与合规事项指定具名责任角色——CTO 为 AI 治理最高管理责任人，各业务部门负责人为本部门 AI 应用第一责任人，数据安全委员会承担跨部门审议职责。公司建立 AI 相关错误与损害的调查处置流程，对因 AI 系统引发的问题及时调查、纠正与补救，并按规定承担相应法律责任；员工发现 AI 系统异常、误用或不当结果应及时按公司上报机制报告。

3.7 明确 AI 应用的边界：公司通过《AI 应用管理办法》等制度明确 AI 的授权使用范围、能力边界与限制条件，形成允许用途与禁止用途清单，并配置相应的护栏（guardrails）与控制点，防止 AI 系统被误用、越界使用或应用于未经批准的场景；AI 系统不得超出其设计用途运行，超出授权范围的使用须重新履行审批程序。

3.8 AI 数据中心与模型的低碳要求：公司将 AI 的生态足迹纳入环境管理范围，要求自建及第三方的 AI 数据中心与模型满足低碳要求：识别并跟踪 AI 算力相关的能源消耗、水资源消耗与碳排放强度；采用算法轻量化、模型压缩与智能任务调度等技术降低算力负载与能源浪费；优先选用高能效、低电能利用效率（PUE）的基础设施并提高清洁电力使用比例，优先选择能源结构中以可再生能源为主的云服务与数据中心供应商；将能效与碳排放要求纳入供应商评估与《供应商行为准则》。

3.9 禁止使用与部署的人工智能系统：公司承诺不开发、不使用、不部署以下类型的 AI 系统：

1. 采用潜意识、刻意操纵或欺骗性技术，实质性扭曲个人行为的 AI 系统；
2. 利用特定群体因年龄、残疾或社会经济状况而产生的脆弱性，实质性扭曲其行为的 AI 系统；
3. 基于社会行为或个人特征对个人进行社会评分（social scoring），导致在无关场景中受到不利对待或产生不成比例、不合理结果的 AI 系统；
4. 用于实时远程生物识别（RBI）监控用途的 AI 系统，以及经公司评估认定违反适用法律法规或与本政策原则存在重大冲突的应用。

四、实施机制

4.1 敏感 AI 能力访问限制：对可能涉及伦理或隐私风险的人工智能能力实行严格的访问控制与授权管理，仅经审批的授权人员可在规定场景下使用；公司不将生物识别能力用于对不特定公众的持续性、系统性监控目的。

4.2 AI 生成内容与 AI 决策结果的标识：对 AI 生成的内容及由 AI 驱动的决策结果予以清晰标识，使接收方能够辨别内容来源性质；在用户交互场景中主动告知其正在与 AI 系统交互。

4.3 模型漂移与退化监测：依托 NEF 系统实时监测能力持续跟踪 AI 模型的运行表现与输出质量，自动完成异常识别与预警；当监测显示模型精度下降或效果退化时，及时采取再训练、参数调整或版本回退等纠正措施，保障系统持续可靠与有效。

4.4 已部署模型的公平性与稳健性评估：对已上线的 AI 模型定期开展系统性的公平性与偏见评估，通过审查、偏见测试与公平性评价检查模型是否对不同群体产生不当差异，并对发现的问题实施整改。

4.5 降低生态足迹的举措：通过算法与算力效率优化、基础设施能效要求、清洁电力使用以及供应商协同等方式，持续降低 AI 运行环节的资源消耗与碳排放，相关实践纳入年度能源管理与碳排放管理工作。

4.6 申诉与救济渠道：为受 AI 决策或结果影响的用户及第三方提供便捷、可及的申诉渠道，相关主体可通过客服热线、官方网站客服入口、客户服务邮箱及书面来函等方式提出异议与救济请求；公司及时受理、定向核查并反馈处理结果，确保处置过程公平、透明、可追溯。

4.7 AI 对可持续性成果影响的量化：将 AI 举措对可持续发展目标的影响纳入指标管理，对能源效率提升、资源节约与



能链智电官方公众号

请扫码关注

碳排放减少等成效开展系统测量与跟踪。；公司系统测量 AI 举措对能源效率和碳排放的影响，相关量化数据在年度 ESG 报告中披露。

4.8 员工 AI 伦理与安全培训：公司面向全体员工开展 AI 伦理规范与安全使用培训并纳入整体培训体系：《AI 应用 TIPS》每日科普专栏融入数据隐私保护、算法公平、AI 输出人工校验、业务使用边界等合规伦理内容，2025 年度刊发 20 期；「AI 思享会」专题分享活动传递人机协同准则与 AI 使用红线，2025 年度举办两场；「AI 伙伴种子队伍」覆盖各业务板块约 15% 的员工，承担一线带教与合规理念传播职责。新入职人员须接受安全与合规使用 AI 的基础培训。

五、独立外部验证

5.1 公司已通过中国信息通信研究院（CAICT）数据安全能力（DSMC）认证，AI 相关的数据治理、安全防护与合规管控能力经独立第三方验证；公司 AI 领域的数据安全管理体系已纳入独立第三方审计范围，审计依据 PCAOB 审计准则相关要求（AS 2201 等），覆盖 AI 系统所依托关键信息系统的访问控制、程序变更、程序开发与计算机运行等控制领域。

5.2 公司参照 ISO/IEC 42001 人工智能管理体系标准持续完善 AI 治理框架与分层分类的 AI 培训体系，并将适时委托具备相应资质的独立第三方机构对 AI 管理体系开展认证审核；公司不使用、不引用已失效或不适用的认证与审计结论。

六、政策评审与持续改进

6.1 公司每年至少对负责任 AI 治理框架开展一次评审，结合技术演进、法规更新与利益相关方反馈进行评估与修订；本政策每三年全面复审一次，修订版按内部规定发布后生效并经董事会批准后重新公开披露。本政策的执行情况、相关绩效数据与培训成效在年度环境、社会及管治（ESG）报告中披露。如本政策内容与法律、法规、规章的强制性规定存在不一致的，以法律法规强制性规定为准。

浙江安吉智电控股有限公司
2026 年 4 月



能链智电官方公众号

请扫码关注